Etudes de fiabilité des systèmes : les processus de Markov sortent de leur réserve mathématique grâce aux BDMP

Marc Bouissou • EDF R&D/MRI • (Marc.Bouissou@edf.fr)

1 Introduction

L'étude de la fiabilité et la disponibilité des systèmes complexes, ayant des capacités de reconfiguration, des redondances passives (fonctionnement en normal/secours), ou d'autres types de dépendances entre composants requiert l'utilisation de modèles comportementaux (ou dynamiques), dans lesquels on modélise explicitement le processus aléatoire qui fait évoluer le système d'état en état, jusqu'à ce qu'il atteigne une catégorie d'états indésirable.
Les BDMP ("Boolean logic Driven Markov Processes" ®) sont un nouveau formalisme graphique permettant de définir aisément de tels modèles. Ils ont de plus des propriétés mathématiques qui facilitent les calculs probabilistes.

2 Avantages des BDMP par rapport aux modèles classiques

Un genre particulier de processus aléatoires, les **processus de Markov**, sont un support idéal pour des développements mathématiques ; ils possèdent des propriétés à la fois simples et très puissantes car aux nombreuses conséquences. Il existe une très abondante littérature scientifique à leur sujet. Un processus de Markov à espace d'états fini peut être défini entièrement par une matrice de nombres réels, telle que le produit $a_{ij}dt$ du terme i,j de la matrice par dt représente la probabilité que le processus passe de l'état i à l'état j en un temps dt. Ces processus ont aussi une représentation graphique sous forme de graphe appelé *graphe de Markov*, commode tant que le nombre d'états à considérer (égal à la dimension n de la matrice) ne dépasse pas la dizaine.

Malheureusement, les processus de Markov souffrent d'une mauvaise image auprès des ingénieurs. Alors que le mathématicien raisonne avec une égale facilité sur une matrice 4x4 représentant un système à deux composants que sur une matrice $2^{100}x2^{100}$ représentant un système à 100 composants, on imagine la détresse de l'ingénieur quand il lui faut faire ce changement d'échelle !

Il existe divers formalismes dotés d'un niveau d'abstraction bien meilleur que les graphes de Markov eux-mêmes, qui permettent de les construire automatiquement. Malgré cela, on est toujours confronté à un phénomène d'explosion combinatoire. Pour faire face à ce problème, on a souvent recours à la simulation de Monte Carlo qui est une méthode à la fois très générale et insensible au nombre d'états. Cependant, les résultats qu'elle produit peuvent être imprécis et demander des temps de calcul prohibitifs pour des systèmes très fiables. Cette limitation de la simulation explique pourquoi les calculs analytiques sur les graphes de Markov, qui sont d'autant plus efficaces que les systèmes sont plus fiables, ont un grand intérêt.

Les graphes de Markov sont bien plus difficiles à **construire, à valider** et à **exploiter** que les modèles dits "statiques", qui font l'hypothèse de l'indépendance des différents processus élémentaires de panne et de réparation associés aux composants. Les **arbres de défaillances** sont le type de modèle statique de loin le plus utilisé par les ingénieurs chargés de faire des études de sûreté de fonctionnement de systèmes, sauf dans quelques domaines spécialisés, tels que les systèmes informatiques, ou les systèmes de production.
Grâce aux BDMP il est possible de spécifier, à l'aide de modèles graphiques **ressemblant fortement aux arbres de défaillances**, des graphes de Markov de très grande taille ; ils apportent un gain sensible vis à vis des trois types de problèmes cités ci-dessus.

Les BDMP permettent de modéliser aisément des systèmes avec des **interactions très variées** entre composants : les reconfigurations et redondances passives, les séquences de démarrage avec conditionnement de chaque étape par la réussite des étapes précédentes, les défaillances corrélées (appelées dans le jargon des fiabilistes les "défaillances de cause commune"), les fonctionnements en plusieurs phases, avec des changements de la mission du système d'une phase à la suivante...
Pour ce qui est de la validation des modèles, les BDMP ont aussi un avantage : comme leur représentation graphique est très proche de celle des arbres de défaillances, ils sont facilement "pris en main" par les fiabilistes,

qui ont l'habitude d'utiliser ce type de modèle. Les BDMP de même que les arbres de défaillances sont lisibles et sont des modèles **hiérarchiques**, permettant divers niveaux d'abstraction.
Enfin, les BDMP permettent une **réduction spectaculaire** de l'explosion combinatoire inhérente à l'utilisation des graphes de Markov. Nous leur avons donné une définition mathématique rigoureuse, ce qui nous a permis de démontrer des théorèmes à leur sujet, prouvant que cette réduction de l'explosion combinatoire ne se fait pas au détriment de la qualité des résultats obtenus. Grâce aux BDMP, on peut gagner **au moins une décade dans la taille en nombre de composants** des problèmes que l'on peut traiter par modélisation markovienne.

Les principales limites des BDMP sont le fait qu'ils sont mal adaptés à la modélisation de systèmes de production (de type chaîne de montage de voitures, raffinerie…) et aux systèmes non cohérents, c'est à dire tels que certaines défaillances puissent "réparer" le système, c'est à dire rétablir la fonction qu'il est chargé d'assurer.

Faute de place, nous ne pouvons pas définir les BDMP dans cet article. Nous allons seulement en donner un exemple très simple, en expliquant ce qu'il représente afin que le lecteur puisse découvrir la facilité de leur utilisation.

3 Un exemple

Soit un système S composé de trois sous-systèmes A, B, C en redondance totale, c'est à dire tels que le fonctionnement d'au moins un des trois suffise à assurer la mission de S. A et B sont en fonctionnement continu, et dès que l'un des deux tombe en panne, on met en œuvre le secours C, mais cela nécessite un certain temps, pendant lequel le système est fragilisé, puisqu'il reste un seul sous-système en fonctionnement. Un tel système peut être représenté par un BDMP obtenu à partir de la **Figure 1** en développant les sous-arbres dont les sommets sont représentés par les portes k/n appelées A_defaillant, B_defaillant, C_defaillant. Ces sous-arbres sont les sous-BDMP que l'on construirait si l'on avait à modéliser indépendamment les sous-systèmes A, B et C, car les BDMP conservent le caractère hiérarchique des arbres de défaillances, ce qui est un avantage fondamental.

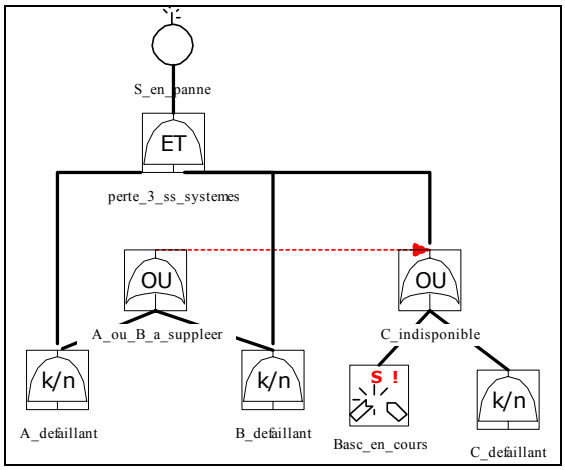

Figure 1 : exemple de BDMP (les portes X_defaillant sont à développer)

Ce modèle se lit ainsi : lorsque A ou B est défaillant, la porte A_ou_B_a_suppleer passe à VRAI, ce qui a pour effet (grâce au lien en pointillés, appelé "**gâchette**") de faire passer les feuilles du sous-arbre C_indisponible du mode "non sollicité" au mode "sollicité". Disons au passage que les gâchettes sont le **seul** élément graphique que l'on trouve dans les BDMP et pas dans les arbres de défaillances classiques.
La feuille Basc_en_cours représente un processus qui met la feuille à VRAI avec une probabilité de 1 lors du changement de mode induit par la défaillance de A ou B. Cette feuille met donc la porte C_indisponible à VRAI tant qu'elle n'a pas été "réparée" : c'est ce qui modélise le temps nécessaire pour mettre le sous-système C en action. Après ce temps, C_indisponible revient à FAUX et garde cette valeur tant que C_defaillant ne passe pas à VRAI (à la suite de défaillances dans le sous-système C). A la réparation du composant qui était initialement tombé en panne, les éléments du sous-système C repassent dans le mode non sollicité. Dans ce mode, on termine les réparations qui étaient éventuellement en cours, mais on ne considère plus les défaillances.

On voit d'après cet exemple que le nombre d'éléments à représenter dans le BDMP est à peu près **proportionnel** au nombre de composants dans le système, alors que le comportement spécifié par le BDMP correspond à un graphe de Markov dont le nombre d'états est une fonction **exponentielle** du nombre de composants.

4 Applications des BDMP

Dans le mode d'emploi de l'outil KB3-BDMP (développé par EDF et commercialisé par la société APSYS) et dans plusieurs articles, nous avons présenté la résolution avec les BDMP de nombreux problèmes de modélisation fréquemment rencontrés dans les études de fiabilité : différents types de redondance passive (simple, en cascade…), report de charge, fonctionnement multiphase, modes de défaillance exclusifs, défaillances de cause commune (DCC) en fonctionnement, DCC fonctionnement-démarrage, évolutions différentes du système selon l'ordre dans lequel certains événements se sont produits, partage de ressources pour les réparations... Grâce au caractère hiérarchique des BDMP, nous avons pu donner la plupart des solutions sous une forme générique, en décrivant seulement quelques portes et gâchettes à placer au sommet du BDMP que l'on doit construire (comme dans l'exemple ci-dessus). Il ne reste plus, pour modéliser un système réel particulier, qu'à développer les événements laissés en suspens dans les modèles suggérés.

En seulement cinq ans d'existence, les BDMP ont déjà servi à la réalisation d'études variées de systèmes industriels complexes : poste électrique de distribution [2], alimentations électriques d'un groupe de serveurs Internet, réseaux électriques d'une usine d'ARCELOR et d'autres usines (imprimerie, alimentaire, micro-électronique...), comparaison de schémas des liaisons d'un champ d'éoliennes en mer, alimentations électriques de l'aéroport de Londres, comparaison de deux politiques d'exploitation des groupes électrogènes diesels en cas de perte de longue durée des alimentations externes dans une centrale nucléaire, système de déclenchement de vannes de sécurité associées à un barrage...

5 Conclusion

Le but de ce court article était de sensibiliser le lecteur à la question de la modélisation par les processus de Markov, et de l'informer de l'existence d'un nouveau type de modèle qui la facilite grandement pour la réalisation d'études de sûreté de fonctionnement.
Sans doute reste-t-il à le convaincre. Pour cela, nous ne pouvons que l'inciter à lire les articles plus techniques et détaillés dont la liste est disponible sur la « homepage » de l'auteur, à l'adresse : http://perso-math.univ-mlv.fr/users/bouissou.marc/.
L'article [1], la référence qui définit formellement les BDMP et démontre leurs propriétés mathématiques, est à garder pour la fin, car c'est le plus ardu.

6 Références

[1] M. BOUISSOU, J.L. BON : **A new formalism that combines advantages of fault-trees and Markov models: Boolean logic Driven Markov Processes,** Reliability Engineering and System Safety, Volume 82, Issue 2, November 2003, Pages 149-163.

[2] J. PESTOURIE, G. MALARANGE, E. BRETON, S. MUFFAT, M. BOUISSOU : **Etude de la sûreté de fonctionnement d'un poste source EDF (90/20 kV) avec le logiciel OPALE,** 14ème congrès de fiabilité et maintenabilité, Bourges, (France), Octobre 2004.